Summary

Report

SUMMARY OF SECURITY CONTROL AUDITS OF
DOD FINANCE AND ACCOUNTING SYSTEMS

Report No. D-2002-015 November 7, 2001

Office of the Inspector General
Department of

Additional Copies

To obtain additional copies of this summary report, visit the Inspector General, DoD Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Evaluations

To suggest ideas for or to request future evaluations, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Evaluation Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
GAO	General Accounting Office
IG	Inspector General
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

November 7, 2001

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Summary of Security Control Audits of DoD Finance and Accounting Systems (Report No. D-2002-015)

We are providing this summary report for your information and use. We summarized systemic control weaknesses identified in prior Inspector General, DoD, reports. We considered management comments on a draft of this report when preparing the final report.

Comments to the draft of this report conformed to the requirements of DoD Directive 7650.3; therefore, no additional comments are required.

For additional information on this report, please contact Ms. Kathryn M. Truex at (703) 604-9139 (DSN 664-9139) (kmtruex@dodig.osd.mil) or Mr. Dennis L. Conway at (703) 604-9158 (DSN 664-9158) (dconway@dodig.osd.mil). See Appendix D for the report distribution. The team members are listed inside the back cover.

Thomas F Gimble

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2002-015 **November 7, 2001**
(Project No. D2001FG-0042)

Summary of Security Control Audits of DoD Finance and Accounting Systems

Executive Summary

Introduction. Congress emphasized the importance of developing and maintaining controls to protect Federal information and information systems in its 2001 Defense Authorization Act. The Act requires DoD to develop a cost-effective security control program that continually assesses risk, is tested and evaluated periodically, and is approved by the Director, Office of Management and Budget. The General Accounting Office has also emphasized the importance of information system security controls, as well as financial management, by placing both of these issues on its 2001 list of Government-wide high-risk areas.

The Defense Finance and Accounting Service is responsible for financial management in DoD and processes payments for about 5.4 million military, civilians, retirees, and annuitants; 14.4 million invoices; and 5.4 million travel payments. The Defense Information Systems Agency provides computer services to the Defense Finance and Accounting Service and processes finance and accounting data on 47 critical finance and accounting systems at 5 computer centers containing 60 large computers.

The Inspector General, DoD, issued 28 audit reports from March 1994 through February 2001 that addressed the effectiveness of security controls over DoD financial data. The 28 reports identified weaknesses in controls over DoD finance and accounting systems.

Objective. The overall objective was to identify systemic general control weaknesses in systems that produce financial information. General controls are the structure, policies, and procedures that apply to an activity's overall computer operations.

Results. Security controls over information systems processing financial data are a systemic problem. Both the Defense Finance and Accounting Service and the Defense Information Systems Agency must have effective security control programs in place to protect DoD finance and accounting systems from potential loss, misuse, or destruction of data.

We determined that DoD finance and accounting systems, relied on to annually process approximately $288 billion in disbursements and more than 100 million accounting transactions, continue to have reoccurring general control weaknesses. While Defense Finance and Accounting Service and Defense Information Systems Agency managers have agreed to over 87 percent of the recommendations in Inspector General audit reports issued during the past 7 years, the same or similar problems were identified during subsequent audits. These problems include weaknesses in security over access to computer data, equipment, and facilities (51 occurrences in 24 reports); security over access to computer systems (26 occurrences in 20 reports); lack of security planning and policies (46 occurrences in 18 reports); inadequate preparation for disasters

(16 occurrences in 10 reports); lack of adequate control over system changes (12 occurrences in 8 reports); and lack of separation of duties (7 occurrences in 7 reports).

The fact that the same or similar weaknesses reoccurred does not necessarily mean corrective actions were not taken. Rather, similar weaknesses may have occurred because of system modifications, relocations and consolidations, reassignment of security personnel, or other mitigating circumstances. However, repetitions of weaknesses do indicate a lack of sustained emphasis on security. Defense Finance and Accounting Service and Defense Information Systems Agency managers should be more aggressive in their oversight roles and in mandating timely and comprehensive system security reviews. This will avoid the further repeat of system security weaknesses that make DoD financial systems vulnerable to unauthorized use, loss, or destruction. See the Finding section of the report for details on the results.

Summary of Recommendations. We recommend that both the Director, Defense Finance and Accounting Service, and the Director, Defense Information Systems Agency, evaluate the comprehensiveness and effectiveness of their existing security review program to identify, track, monitor, and resolve general control weaknesses, and establish performance metrics to evaluate the effectiveness of the security programs.

Management Comments. The Director for Information and Technology, Defense Finance and Accounting Service, concurred with the recommendations. The Director stated that the Service is working on establishing processes and procedures to review the certification and accreditation of its systems. Also, the Service is making modifications, to be completed by October 2001, that will improve the ability for tracking the status of system certifications and accreditations. In addition, the Director stated that the Service has recognized the need for performance metrics in assessing its security program and is participating in the DoD Information Assurance Readiness Metrics Working Group. This Group was established to research, develop, and validate metrics for use in the information assurance readiness assessment process.

The Inspector General, Defense Information Systems Agency, concurred with the recommendations. The Agency's Inspector General stated that an evaluation will be conducted to assess the existing security review program with expected completion by March 31, 2002. Also, the Inspector General stated that performance metrics have been established which allow the Chief Information Officer to measure the effectiveness of the security program.

Response. Management's comments are responsive to the intent of the recommended actions. Refer to the Finding for a discussion of management comments and to the Management Comments section for a complete text of the comments.

Table of Contents

Background

Security Over DoD Systems. Information systems are as crucial to DoD management activities as the central nervous system is to the human body. Managers at all levels depend on information that is compiled, analyzed, adjusted, and reported with automated systems. The magnitude of DoD spending on information technology exceeds $20 billion annually. DoD financial and accounting systems process approximately $288 billion in disbursements annually.

Unauthorized access to computer networks poses a multifaceted threat to national security that cuts across boundaries and can cause problems in virtually all economic sectors and levels of Government. This threat is both internal and external, and constantly evolving. Perpetrators can include disgruntled or irresponsible employees, criminals, hobbyist hackers, agents of hostile states, and terrorists.

Management and Oversight of Systems and Security. Security over Federal information systems continues to be an increasingly dominant concern to the President, Congress, and DoD officials who have initiated legislation and directives to require management and oversight of information systems and information security.

Presidential Decision Directive 63. The President issued Presidential Decision Directive 63 (Executive Order 13010) on July 15, 1996. A subsequent document, "Protecting America's Critical Infrastructure: PDD 63," May 22, 1998, outlined the established goals for achieving a reliable, interconnected, and secure information system network by 2003 and for significantly increasing system security by 2000.

Congressional Emphasis on Information System Controls. Congress passed the Government Information Security Reform Act, Public Law 106-398, October 30, 2000, to emphasize the importance of developing and maintaining controls to protect Federal information and information systems. The Act tasked agencies to be responsible for ensuring the integrity, confidentiality, and authenticity of information and information systems by assessing information security risks, testing security controls, and training personnel with significant responsibility for information security.

The Act further requires that an agency perform an independent review of its information security program each year. Each agency's Inspector General or an independent activity should conduct the review. Agencies should report the results to the Director, Office of Management and Budget (OMB). The Director, OMB, will report annually to Congress on the status of security programs for all agencies.

Congressional Investigations on Computer Security. The General Accounting Office (GAO), the investigative arm of Congress, has continued to recognize computer security as a Government-wide high-risk area since 1997.

In a September 2000 report, "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies," GAO/AIMD-00-295, September 6, 2000, GAO pointed out that the increase in interconnectivity poses significant risk to computer systems, operations, and networks. Without proper controls, it is possible for individuals to interfere with or eavesdrop from remote locations for purposes of fraud or sabotage.

Then GAO issued a report, "Major Management Challenges and Program Risks: Department of Defense," GAO-01-244, in January 2001. The report pointed out that despite both the GAO and the Inspector General (IG), DoD, reports, poor management of security programs was an underlying cause of weaknesses in the protection of computer security. In addition, the GAO report states that although DoD has taken steps to improve computer security, recent IG, DoD, audits continue to indicate that much more needs to be done to implement a robust information security program in an effort to manage and prevent these potential threats.

Defense Management Challenges. With regard to financial management, DoD continues to be unable to comply with legislation for auditable annual financial statements including Public Law 101-576, "Chief Financial Officers Act of 1990," November 15, 1990. DoD continues to cite the root problem as being the lack of modern, integrated information systems, and unreliable financial data. DoD estimates spending at least $3.7 billion for FY 2000 through FY 2003 to make system improvements. The improvements needed include system controls to comply with the Computer Security Act of 1987 and OMB Circular No. A-130 Revised, "Management of Federal Information Resources," November 30, 2000.

The Deputy Inspector General, DoD, included financial management and systems security in the top 10 management challenges facing the DoD, in testimony on February 17, 2000, to the House of Representatives Committee on Budget. The Deputy Inspector General, DoD, repeated these challenges in testimony about Defense management issues on February 12, 2001, before the Senate Committee on the Budget.

More recently, the Secretary of Defense contracted with the Institute for Defense Analysis to study and recommend strategy for financial management improvement within the department. The Institute issued a report, "Transforming Department of Defense Financial Management, A Strategy for Change, Final Report," April 13, 2001, which recommends an approach for senior leadership to give high priority to the goal of relevant, reliable, and timely financial information.

DoD Audits on Security of Financial Systems. The IG, DoD, issued the 28 audit reports that we selected for review that addressed security and controls over DoD financial management systems and the need for better security over those systems. In some cases, the same or similar weaknesses were identified in the subsequent audits of the same or similar systems. These weaknesses reoccurred despite management actions taken to correct the problems. Corrections of the weaknesses are the responsibility of the system owners, the

Defense Finance and Accounting Service (DFAS), as well as the Defense Information Systems Agency (DISA) which operates the computers that process financial data for DFAS.

This report summarizes the past audit reports on finance and accounting systems, to highlight that while DoD Components have been responsive in their efforts to correct identified weaknesses, weaknesses continue to reoccur. The weaknesses summarized in this report focus on general controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. Normally, if general controls are weak, the reliability of controls associated with the input, processing, and output of data (commonly referred to as application controls) is diminished. For this reason, general controls are usually evaluated separately from and prior to evaluating application controls. When general controls are deemed weak, additional audit work is generally not performed to assess application controls. As such, the IG, DoD, has performed limited audits on application controls and this report addresses only general controls.

Objective

The objective was to identify systemic general control weaknesses in systems that produce financial information. See Appendix A for discussion of the scope and methodology.

Security Controls Over DoD Financial Systems

In spite of 28 audit reports, and agreements by the Defense Finance and Accounting Service and the Defense Information Systems Agency to implement over 87 percent of the recommended corrective actions, DoD finance and accounting systems continued to have reoccurring general control security weaknesses. These weaknesses reoccurred because the Defense Finance and Accounting Service and the Defense Information Systems Agency did not have sufficiently rigorous programs to implement general controls and effectively monitor for general control weaknesses. As a result, financial information that DoD managers rely on may not be complete and accurate. Further, the information could be vulnerable to unauthorized use, loss, or destruction.

Controls in Financial Management Systems

System of Management Controls. OMB Circular No. A-127, Revised, "Financial Management Systems," July 23, 1993, states that financial management systems are to include a system of management controls which ensures that the use of an agency's resources is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data are obtained, maintained, and disclosed in reports.

Also, OMB Circular No. A-127 states that agencies are to plan for and include security controls in financial management systems in accordance with OMB Circular No. A-130 Revised, "Management of Federal Information Resources," November 30, 2000.

Minimum Set of Information Security Controls. OMB Circular No. A-130 establishes a minimum set of controls to be included in automated information security programs. The GAO refers to this minimum set of controls as general and application controls.

General controls are the policies and procedures that apply to an activity's information systems and help to ensure proper operation. General controls should address:

- limiting access to computer resources such as data, equipment, and facilities (access controls);
- establishing controls to monitor and limit access to computer programs and sensitive files that control the computer equipment and the software (system software controls);
- establishing an overall security program (entity-wide security);

- establishing procedures for preventing disruptions in service to customers (service continuity);

- implementing procedures for developing and changing computer software (application change controls); and

- separating duties so that unauthorized or fraudulent activity can be prevented or better detected (segregation of duties).

See Appendix B for a more detailed definition of these major categories of general controls.

Federal Requirement to Review System Controls. The Chief Financial Officers Act of 1990, and the Federal Financial Management Improvement Act of 1996, Public Law 104-208, September 30, 1996, require that controls over automated information systems be evaluated. The controls must be evaluated to determine the reliability of data processed through systems and subsequently recorded in financial statements. When controls are not sufficient and vulnerabilities remain unresolved, auditors will not be able to rely on computer-processed data supporting the financial statements without substantial verification and tests. Further, managers may make decisions based on inaccurate or unreliable data.

Reliability of Controls Over Finance and Accounting Systems

General Controls Over Systems. DoD finance and accounting systems, relied on to annually process approximately $288 billion in disbursements and more than 100 million accounting transactions, continue to have reoccurring general control weaknesses. We reviewed 28 audit reports issued by the IG, DoD, over the past 7 years[1] that identified general control weaknesses that relate to the security and reliability of DoD financial systems. DoD managers can be commended for agreeing to take corrective action on over 87 percent of the recommendations that relate to the identified weaknesses (189 of 215 recommendations) in the audit reports. However, in many instances the same or similar general control weaknesses were identified during subsequent audits of the same or other DoD financial systems.

Some of the 28 IG, DoD, reports summarized in this report identified more than one weakness in a general control category. Not all weaknesses had related recommendations, while some weaknesses had more that one related recommendation.

[1] The 28 reports were issued from March 18, 1994, through February 28, 2001.

The following table shows the types of and number of general control weaknesses identified in IG, DoD, audit reports. Although not shown in the table, some reports contain multiple occurrences of the same type of weakness.

IG, DoD, Audit Report Number *	IG, DoD, Audit Reports with General Control Weaknesses					
	Type of General Controls					
	Access	System Software	Entity Wide	Service Continuity	Application Changes	Segregation of Duties
94-060	X		X		X	
94-065		X			X	
95-066	X	X				
95-263	X	X				
95-270	X	X		X	X	X
96-053		X				
96-124	X	X	X	X	X	
96-175	X		X			
96-179	X	X				
97-050	X	X				
97-203	X	X	X			
98-007	X		X			
98-038					X	
98-054	X	X	X			
98-098	X		X	X		
99-107	X		X			X
99-128	X	X	X			
99-225	X	X	X	X		X
99-233	X	X	X			
00-008	X	X	X		X	
D-2000-096	X	X	X	X		
D-2000-139	X					
D-2000-182	X	X	X	X		X
D-2001-029	X	X	X			
D-2001-044		X	X	X		
D-2001-052	X	X	X	X		X
D-2001-055	X		X	X	X	X
D-2001-068	X	X		X	X	X
Number of Reports with Weaknesses	24	20	18	10	8	7

*Beginning in January 2000, the DoD audit agencies started a new method for numbering audit reports. The "D" preceding the year in the table above indicates that the report was issued by the IG, DoD.

The following examples are typical of general control weaknesses identified in the audit reports for the past 7 years.

Controls Over Access to Systems. Of the 28 IG, DoD, reports, 24 reports identified 51 occurrences of security weaknesses in controls over access to those systems. Access controls are designed to limit or detect access to computer systems, thereby protecting those systems against unauthorized access that could result in the modification, loss, or disclosure of information contained within those systems.

Granting Access to System Files. IG, DoD, Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System-Reserve

Component," August 13, 1997, identified over 170 personnel that were granted access to system files to perform sensitive tasks such as terminating computer jobs and altering priorities for job processing. This military payroll system paid $3.7 billion to the Army and Air Force Reserves and the National Guard in FY 1996. Such access should be monitored and restricted only to personnel with a need to know the information in the system. Otherwise, users could manipulate the system without detection, and the integrity of the data may not be safeguarded.

Access to Data Files. IG, DoD, Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999, reported that more than 4,100 users had access to the civilian pay system despite not having used or accessed the system in over 90 days. The Defense Civilian Pay System processed $35 billion in payroll transactions annually for more than 700,000 employees. Inactive or infrequent user access leaves an open door for individuals seeking unauthorized entry into a system.

Controls Over Passwords. IG, DoD, Report No. 98-054, "Compilation of FY 1996 Air Force Consolidated Financial Statements at the Defense Finance and Accounting Service Denver Center," January 23, 1998, reported that system managers did not control access to the Chief Financial Officer Reporting System. Specifically, no requirement existed that passwords be greater than six alphanumeric characters or that passwords be changed at least annually. In addition, system users could delete the need for a password altogether to obtain quicker access.

We cited another example of poor controls over passwords in IG, DoD, Report No. D-2000-182, "Data Processing Control Issues for the FY 1999 Military Retirement Fund," August 31, 2000. The report stated that several hundred users at the Chambersburg Detachment of the DISA Defense Enterprise Computing Center in Mechanicsburg, Pennsylvania, had passwords that were not set to expire at all.

Allowing users to ignore password protective measures, such as making passwords a minimum length, or periodically changing passwords, provides the opportunity for unauthorized persons to access the system and data without being tracked. Further, failure to regularly change passwords increases the risk that a user's password may be compromised and used for unauthorized purposes.

Access Monitoring and Review. IG, DoD, Report No. D-2001-029, "General Controls Over the Electronic Document Access System," December 27, 2000, reported that, because of staffing shortages, the information security manager had not developed an overall plan to review security for the Electronic Document Access System. (The system processes 82,000 contract payments per month.) As a result, an intruder gaining sufficient access to potentially commit fraud or perform malicious acts could do so without timely detection.

System Software Controls. Of the 28 reports, 20 addressed weaknesses in controls over the software in a system. The 20 reports identified

26 occurrences. System software controls are similar to access controls; however, system software controls monitor and limit access to computer programs and sensitive files that control the computer equipment and the software, as compared to access controls that monitor and limit access to computer resources such as data, equipment, and facilities. Inadequate controls over system software could result in unauthorized individuals reading, modifying, or deleting critical or sensitive information and programs. In addition, weaknesses in system software controls seriously diminish the reliability of information produced by the computer system and increase the risk of fraud and sabotage.

Use of System Security Software. IG, DoD, Report No. 97-050, "Evaluation of Controls Over Workflow Applications Selected for Electronic Document Management," December 17, 1996, reported that security controls over the Electronic Document Management system needed improvement. The Electronic Document Management system facilitates the indexing, storage, and processing of more than 4 million documents. Testing of the Electronic Document Management system determined that the system did not have a security software program in place to control access.

An effective security software program would demonstrate the security needed over log-on procedures, the ability of the system to maintain user audit trails, and the security needed to protect system data files. These are standard features of security software programs available and in wide use; and are requirements of DoD system security policy. Lack of security software programs that control access hampers the system administrator and other security personnel in maintaining protection over their systems.

Controls Over Access to System Software. IG, DoD, Report No. D-2000-096, "Information Technology General Controls for the Standard Automated Materiel Management System," March 7, 2000, reported that security over the system libraries[2] for the Standard Automated Materiel Management System was deficient at the DISA Defense Enterprise Computing Center in Columbus, Ohio. Because the system libraries had not been reviewed and closely monitored, 6 could not be found and 28 contained duplicate files and inconsistent versions of the libraries. A system's libraries are very sensitive and corruption of those libraries could allow the computer to continue processing transactions, but with potentially unexpected results.

Entity-Wide Security. Organizations such as DFAS and DISA should have entity-wide security programs in place to provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the organization's computer-related controls. Without a well-designed program, security controls may be inadequate, responsibilities may be unclear, misunderstood, and improperly implemented, and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for

[2] A library is a collection of computer files that controls how a computer processes transactions.

controls over low-risk resources. Of the 28 IG, DoD, reports we reviewed, 18 identified 46 occurrences of weaknesses related to entity-wide security.

Responsibility for Security. IG, DoD, Report No. 99-233, "General Controls for the General Accounting and Finance Systems," August 17, 1999, reported that DFAS could not ensure that the information system security officers could effectively execute the security program. (The General Accounting and Finance System processes about $125 billion in Air Force transactions annually.)

The information system security officers were unable to effectively monitor or enforce security over the General Accounting and Finance System because they had not received training on the automated security software program used to control access to the system. In addition, the information system security officers' positions within the organization placed them under the system manager. As such, the security officers did not have the appropriate authority and independence to carry out security duties.

The weaknesses identified in the General Accounting and Finance System report are similar to weaknesses regarding the role of the information system security officer identified in IG, DoD, Report No. 99-107 "Computer Security for the Defense Civilian Pay System," March 16, 1999. In that report, the information system security officer again did not have the level of authority or the independence to enforce security policy.

Training. IG, DoD, Report No. 98-007, "General and Application Controls Over the Mechanization of Contract Administration Services System," October 9, 1997, reported that 27 percent of terminated or resigned employees still were authorized to have access to sensitive data within the system. These employees still had access because system security officers lacked training on removing user identification codes or user access to sensitive system files at the end of a job assignment or employment. The Mechanization of Contract Administration Services System facilitates payment authorizations and administration processing of over 387,000 contracts valued at $810 billion. Because of the weak security controls, contract and payment data were vulnerable to inappropriate access.

Security Planning. IG, DoD, Report No. D-2001-029, "General Controls Over the Electronic Document Access System," December 27, 2000, concluded that DFAS lacked a security plan and had not conducted an assessment of the risk involved in electronically transmitting documents, such as contracts and invoices, rather than using traditional paper. Electronic document access, as planned, would be available to 15,000 users to process 82,000 contract payments per month. The absence of a security plan and risk assessment increases the risk that data transmitted and maintained in the system could be altered or misused and that verification of the transactions could be labor intensive and administratively burdensome.

Security Monitoring. IG, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," February 15, 2001, stated that DFAS security officers had not monitored reports available from the security software that listed security violations. Because personnel had not reviewed reports containing almost 20,000 instances of unauthorized accesses, the reliability of the data in the system was decreased and the risk of destruction or disclosure of data was increased.

As another example, IG, DoD, Report No. D-2000-096, "Information Technology General Controls for the Standard Automated Materiel Management System," March 7, 2000, stated that DFAS had not performed re-investigations for 5 of 16 employees sampled. Re-investigations are a means to ensure that personnel with access to sensitive information continue to merit that access. A result of untimely re-investigations is that those employees may have had inappropriate access to information, not just in the system, but throughout the organization. The Standard Automated Materiel Management System performs accounting for the Defense Logistics Agency's operations that includes 4 million items, valued at $9 billion, and sales of $11.4 billion.

Continuity of Operations. Service continuity controls ensure that when unexpected events occur, critical operations continue with a minimum of interruption or are promptly resumed, and that critical and sensitive data and programs are protected. Of the 28 audit reports, 10 identified 16 occurrences of weaknesses in service continuity controls.

Planning for Unexpected Events. IG, DoD, Report No. 96-124, "Selected General Controls Over the Defense Business Management System," May 21, 1996, reported that the DISA Defense Enterprise Computing Center at Columbus, Ohio, was not adequately prepared to react in the event of a disaster. Specifically, the DISA center had not sufficiently analyzed risks for catastrophic events, prepared detailed disaster recovery plans, backed up data files at an off-site storage location, or tested recovery plans. The plan for the center was dated 1990, but the center really did not have a plan. Four years later, IG, DoD, Report No. D-2000-096 again cited the lack of an updated plan. The plan, dated 1997, had not been changed to reflect the modifications to the operations environment at the center. Consequently, a disaster could interrupt computer service and cause a loss of procurement, personnel, pay, and logistics data at that DISA center.

Disaster Recovery Plans. Both IG, DoD, Report No. D-2001-052, "Controls Over the Defense Joint Military Pay System," and IG, DoD, Report No. D-2001-055, "General Controls for the Defense Civilian Pay System," February 21, 2001, identified weaknesses in the disaster recovery planning for military and civilian payroll functions. These systems process more than 7.4 million payroll transactions each month and approximately $86.5 billion in payments each year. Specifically, the Defense Joint Military Pay System report cited a lack of planning for relocation, should that be necessary, and a lack of prioritization between the Defense Joint Military Pay System and other functions within the operating centers. The Defense Civilian Pay System report stated that the disaster recovery plans had not been tested. Testing is necessary to ensure that personnel are aware of their respective roles, and that the plan, as written, is executable.

Application Software Development and Change Control. Establishing controls over developing and changing software helps to prevent unauthorized programs or unauthorized modifications from being put into use. Without proper software development and change controls, an increased risk exists that irregularities or malicious code could be entered into a system. Of the 28 IG, DoD, reports reviewed, 8 identified 12 occurrences of weaknesses in controls over developing and changing software.

Software Change Approval Process. IG, DoD, Report No. 96-124, "Selected General Controls Over the Defense Business Management System," May 21, 1996, showed that DFAS was not adequately controlling changes being made to software to ensure that only authorized changes were made. This weakness had occurred because managers were not reviewing and authorizing programmer changes to the system's computer code to ensure that only authorized changes were made. Also, procedures for authorizing the movement of software changes from one location to another location did not prevent unauthorized changes. As a result, DFAS managers did not know whether any of the system's programs, which consisted of 2.1 million lines of computer code, contained unauthorized code.

Problem Resolution and Tracking. IG, DoD, Report No. 00-008, "Data Processing Control Issues for the Military Retirement Trust Fund," October 14, 1999, stated that the Denver Detachment of the Defense Enterprise Computing Center at Columbus, Ohio, had between 250 and 275 reports of uncorrected computer processing problems and that several were over a year old. In addition, the Chambersburg Detachment of the Defense Enterprise Computing Center in Mechanicsburg, Pennsylvania, had 311 reports of uncorrected problems, but it appeared that the problems had been fixed, but not logged into the tracking system. It is important to address and resolve computer-processing problems promptly to better ensure that the system is functioning properly and to increase user satisfaction.

In a subsequent report, IG, DoD, Report No. D-2001-068, "Inspector General, DoD, Oversight of the Audit of the FY 2000 Military Retirement Fund Financial Statements," February 28, 2001, weak policy over change controls was reported again. This report stated that the in-house developed tracking system did not have the features and controls that were available from commercial off-the-shelf products. Also, proper and consistent documentation requirements were not being met.

Segregation of Duties. The objective of segregating duties is to ensure that unauthorized or fraudulent activity can be precluded and better detected. Proper segregation of duties is accomplished by ensuring that no one individual is in a position to control key aspects of computer-related operations. By segregating duties, an organization can diminish the likelihood that errors or wrongful acts will go undetected because the actions taken by one individual will serve as a check on the actions of another individual. Seven of the 28 IG, DoD, reports identified weak controls over the segregation of duties.

System Administration. IG, DoD, Report No. 99-225, "Electronic Data Processing General Controls for the Defense Property Accountability System," July 29, 1999, reported that duties of the system administrator and the database administrator were not properly segregated. These conditions existed at the Dayton Detachment of the DISA Defense Enterprise Computing Center in Ogden, Utah. The Defense Property Accountability System is used to account for all property for the DoD. In FY 1998, the value of those properties was $126.2 billion. The lack of segregation of duties allowed the system administrator and database administrator to potentially perform each other's duties. Hence, they could create transactions without accountability within the system.

Programming Staff. In a subsequent report, IG, DoD, Report No. D-2001-068, "Inspector General, DoD, Oversight of the Audit of the FY 2000 Military Retirement Fund Financial Statements," February 28, 2001, we observed that two computer programmers had access to both data files and programs. Allowing programmers to have access to both types of computer resources could result in unauthorized and faulty code being introduced into the system. As a compensating control, management could have instituted and enforced the reviewing of action logs (audit trails) for the programmers; however, that was not done either. Segregation of duties depends on the elimination of opportunities to conceal errors or irregularities; thus, assignment of work should be such that no one individual controls all phases of an activity or transaction.

Systemic Weaknesses Identified in Multiple Systems. Both DFAS and DISA management have been diligent in taking steps to address the weaknesses identified in the 28 reports. However, those efforts were not sufficient to preclude the same or similar weaknesses from reoccurring. In the 28 reports, we identified the following examples of common or systemic weaknesses in multiple systems:

- weaknesses in security over access to data, equipment, or facilities - 51 occurrences in 24 reports;
- weaknesses in security over access to the computer system - 26 occurrences in 20 reports;
- lack of security planning and policies - 46 occurrences in 18 reports;
- inadequate preparation in event of disasters - 16 occurrences in 10 reports;
- lack of adequate control over system changes - 12 occurrences in 8 reports; and
- lack of segregation of duties - 7 occurrences in 7 reports.

Recurring Weaknesses in the Same System. The following are examples where the same or similar weakness was reported in subsequent reports of the same system.

Military Pay. IG, DoD, audit reports on the Defense Joint Military Pay System (Report Nos. 96-175, 97-203, and D-2001-052), repeated general control weaknesses such as the lack of adequate entity-wide security policies and planning, inadequate security control over access, and too little security over the system software. While management repeatedly indicated that actions would be taken in 1996 and in 1997, we identified the same or similar weaknesses again in 2001.

Retirement Pay and Military Retirement Trust Fund. IG, DoD, audit reports on the Defense Retirement and Annuity System (Report Nos. 98-098, 00-008, and D-2000-182) repeated general control weaknesses in access controls, and in the lack of entity-wide security. While management indicated that corrective action would be taken in 1998, the same or similar problems were again cited in reports issued in FY 2000.

Rigor of System Security Controls Programs

The weaknesses identified in the 28 reports reoccurred because DFAS and DISA did not have sufficiently rigorous programs to implement general controls and effectively monitor for general control weaknesses. The 28 reports not only demonstrated repetition in the general control weaknesses identified, but also demonstrated that the causes for the weaknesses were similar for multiple systems. For example, the following were typical causes cited in the reports:

- outdated or incomplete system security programs or plans;
- inadequately trained security personnel;
- limited implementation of automated system security tools;
- noncompliance with DoD security regulations and guidance;
- insufficient emphasis on security and security oversight; and
- ineffective testing, monitoring, and review of security programs.

It should be noted that DFAS and DISA were conscientious in attempting to address weaknesses identified in the reports. In fact, DFAS and DISA agreed to over 87 percent of the recommendations for corrective action related to the weaknesses we identified. Therefore, in some cases, the repetition of security weaknesses may be attributed to system changes or upgrades, changes to security personnel, or other extenuating circumstances, and not attributable to a lack of management action.

Current Oversight Guidance. DoD has issued guidance, as well as designated responsibility for establishing, testing, and monitoring security controls over DoD systems and accrediting those systems with appropriate controls in place.

For example,

- DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, provides mandatory, minimum, security requirements, and requires the heads of DoD components to implement and maintain an overall system security program.

- DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997, establishes system certification and accreditation as the standard DoD process for identifying information security requirements, providing security solutions, and managing system security activities.

- DISA Instruction 630-230-19, "Automated Data Processing Information Systems Security Program," July 9, 1996, describes the use of security readiness reviews to identify and correct security vulnerabilities in support of DITSCAP requirements.

- DFAS Regulation 8000.1-R, "Information Management Policy and Instructional Guidance," version 5.0, July 18, 2000, implements DoD Directive 5200.28 and delegates responsibility for system security to the designated approving authorities,[3] the information security manager, and the security staff.

However, in spite of the guidance and delegation of responsibilities, and efforts by DFAS and DISA to address identified weaknesses, weaknesses continued to be reported. Further, the repetition of similar causes for the weaknesses indicates that systemic causes exist and the implementation of existing guidance has not been sufficiently rigorous. Managers at both organizations need to be more aggressive in their oversight roles to ensure timely and comprehensive system reviews and avoidance of repeat or systemic security weaknesses.

Impact of Adequacy of General Controls Over Systems

DoD has become increasingly dependent on computerized information systems to carry out its operations and to process, maintain, and report essential information. Consequently, the reliability of computerized data and the systems that process, maintain, and report those data are major concerns. Therefore, general controls must be effective to help ensure the reliability, confidentiality, and availability of critical automated information. The fact that IG, DoD, reports continued to identify similar general control weaknesses in more than one system or in the same system more than once, indicates that both DFAS and DISA can do more to provide robust security over DoD financial systems.

[3] Designated approving authorities are senior DoD officials responsible for accrediting each automated information system under their supervision and ensuring compliance with automated information security requirements.

Without effective security controls over systems, DoD managers may not be able to rely on the financial information contained in or produced by those systems. Without adequate controls, those managers cannot be assured that the information is complete and accurate. In addition, without sufficient controls, the systems and information contained within the systems could be vulnerable to unauthorized use, loss, or destruction.

Ensuring that DoD financial systems include sufficient security controls will also assist in addressing requirements of the Government Information Security Reform Act of 2000 and the DoD-wide initiative to bring finance and accounting systems into compliance with the Chief Financial Officers Act of 1990.

Government Information Security Reform Act. The Government Information Security Reform Act of 2000 requires that DoD report annually on the security posture for its critical systems. The first report is due to OMB by October 31, 2001, and should include an assessment of the security risks and tests of security controls. The security program should include performance metrics or measures in order to assess the effectiveness of the program. The IG, DoD, is required to provide an independent assessment of the DoD security program. Reports such as those cited in this summary report will provide support for the IG, DoD, assessment.

Chief Financial Officers Act of 1990. DoD continues to strive to obtain a favorable audit opinion on its financial statements in conformance with the Chief Financial Officers Act. The reliability of the more than 167 systems that provide the information to the financial statements is critical to achieving a favorable opinion. Specifically, the systems' general controls are important to the financial statements to ensure the accuracy, completeness, and reliability of the systems and the financial data within the systems used for the financial statements.

In January 2001, the Under Secretary of Defense (Comptroller) approved the Financial and Feeder System Compliance Process to ensure that each critical financial management and feeder system is compliant with applicable Federal financial management requirements, including OMB Circular No. A-130. The OMB Circular requires security for systems, commensurate with the risk of the harm that could result from the loss, misuse, or unauthorized access. Therefore, to effectively meet the requirements of the Financial and Feeder System Compliance Process, DFAS and DISA must conform to the OMB Circular as well as demonstrate that sufficient general controls are in place for financial systems.

Senior level management must take a more proactive role over system security in order for DoD to reach its goals for financial management and accounting, and information system security. DFAS and DISA managers need to establish a more rigorous program to not only identify and resolve general control weaknesses, but a program to prevent the reoccurrence of weaknesses. Such a program should also include meaningful metrics or measurements to monitor and track the effectiveness of the security program.

Recommendations and Management Comments

1. We recommend that the Director, Defense Finance and Accounting Service:

a. Evaluate the comprehensiveness and effectiveness of its existing security review program to identify, track, monitor, and resolve new and reoccurring general control weaknesses.

b. Establish performance metrics or measures to evaluate the effectiveness of the security program.

Management Comments. The Director for Information and Technology, Defense Finance and Accounting Service, concurred and stated that:

- processes and procedures for reviewing the certification and accreditation of systems are being established, with expected completion by October 2001, to include modifying the system that tracks certifications and accreditations; and

- performance metrics for assessing the Service's security program are needed and personnel are participating in the Information Assurance Readiness Metrics Working Group led by the Defense Information Assurance Program to develop metrics.

2. We recommend that the Director, Defense Information Systems Agency:

a. Evaluate the comprehensiveness and effectiveness of its existing security review program to identify, track, monitor, and resolve new and reoccurring general control weaknesses.

b. Establish performance metrics or measures to evaluate the effectiveness of the security program.

Management Comments. The Inspector General, Defense Information Systems Agency, concurred and stated that:

- on or about September 15, 2001, the DISA Inspector General will begin an evaluation of the existing security review program to be completed by March 31, 2002; and

- performance metrics have been established which allow the Chief Information Officer to measure the effectiveness of the security program.

Appendix A. Summarization Process

Scope

Work Performed. This report summarizes information system security weaknesses identified during 28 audits of DoD computer systems that produce financial information. The 28 audit reports were selected judgmentally from 418 financial-related audit reports issued by the Office of the Inspector General, DoD, from March 1994 through February 2001. We analyzed the reports to determine if weaknesses were related to system security, and if the weaknesses had been identified in prior reports. We also reviewed management's comments that related to the weaknesses to determine if management concurred with the recommendations.

The recommendations for correction of the weaknesses identified in the audit reports were directed to DFAS and DISA. A list of the 28 reports is included in Appendix C.

DFAS is responsible for financial management in DoD and processes payments for about 5.4 million military, civilians, retirees, and annuitants; 14.4 million invoices; and 5.4 million travel payments. DISA provides computer services to DFAS and processes finance and accounting data on 47 critical finance and accounting systems at 5 computer centers containing 60 large computers.

Limitations to Scope. We did not review the management control program at DFAS or DISA because management controls were reviewed and discussed in the prior reports summarized for this report.

Methodology

Use of Computer-Processed Data. We did not use computer-processed data in performing this evaluation.

Evaluation Type, Dates, and Standards. We summarized 28 financial-related audit reports issued by the Office of the Inspector General, DoD, from March 1994 through February 2001.

Appendix B. Major Categories of General Controls

There are six major categories of general controls as follows:

Access Controls. Access controls limit or detect access to computer resources (such as data, equipment, and facilities); thus, they protect those resources against unauthorized modification, loss, or disclosure.

System Software Controls. System software controls limit and monitor access to the powerful programs and sensitive files that control the computer equipment and secure computer programs that the system supports.

Entity-Wide Security. The entity-wide security program should provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the organization's computer-related controls.

Application Change Controls. Application software development and change controls prevent unauthorized programs or modifications to existing programs from being implemented.

Service Continuity. Service continuity controls ensure that, when unexpected events occur, critical operations continue without interruption or are promptly resumed and that critical and sensitive data are protected.

Segregation of Duties. Duty segregation includes policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations that would allow that person to conduct unauthorized actions or gain unauthorized access to assets or records without detection.

Appendix C. Audit Reports on Security Controls

Audit Report No.	Audit Title
94-060	General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization (March 18, 1994)
94-065	Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service (March 24, 1994)
95-066	Controls Over Application Software Supporting the Navy's Inventories Held for Sale (Net) (December 30, 1994)
95-263	Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (June 29, 1995)
95-270	Corrective Actions on System and Software Security Deficiencies (June 30, 1995)
96-053	Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (January 3, 1996)
96-124	Selected General Controls Over the Defense Business Management System (May 21, 1996)
96-175	Computer Security Over the Defense Joint Military Pay System (June 25, 1996)
96-179	Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania (June 27, 1996)
97-050	Evaluation of Controls Over Workflow Applications Selected For Electronic Document Management (December 17, 1996)
97-203	Application Controls Over the Defense Joint Military Pay System Reserve Component (August 13, 1997)
98-007	General and Application Controls Over the Mechanization of Contract Administration Service System (October 9, 1997)
98-038	Control of Database Applications at the Defense Finance and Accounting Service Indianapolis Center (December 12, 1997)
98-054	Compilation of FY 1996 Air Force Consolidated Financial Statements at the Defense Finance and Accounting Service Denver Center (January 23, 1998)
98-098	Selected General Controls Over the Retiree and Casualty Pay Subsystem at the Defense Finance and Accounting Service Cleveland Center (March 30, 1998)

Audit Report No.	Audit Title
99-107	Computer Security for the Defense Civilian Pay System (March 16, 1999)
99-128	Computer Security for the Defense Civilian Pay System (April 8, 1999)
99-225	Electronic Data Processing General Controls for the Defense Property Accountability System (July 29, 1999)
99-233	General Controls for the General Accounting and Finance System (August 17, 1999)
00-008	Data Processing Control Issues For the Military Retirement Trust Fund (October 14, 1999)
D-2000-096	Information Technology General Controls for the Standard Automated Materiel Management System (March 7, 2000)
D-2000-139	Controls Over the Integrated Accounts Payable System (June 5, 2000)
D-2000-182	Data Processing Control Issues For the FY 1999 Military Retirement Fund (August 31, 2000)
D-2001-029	General Controls Over the Electronic Document Access System (December 27, 2000)
D-2001-044	Accreditation Policies and Information Technology Controls at the Defense Enterprise Computing Center Mechanicsburg (February 9, 2001)
D-2001-052	Controls Over the Defense Joint Military Pay System (February 15, 2001)
D-2001-055	General Controls for the Defense Civilian Pay System (February 21, 2001)
D-2001-068	Inspector General, DoD, Oversight of the Audit of the FY 2000 Military Retirement Fund Financial Statements (February 28, 2001)

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Defense Finance and Accounting Service
Defense Information Systems Agency

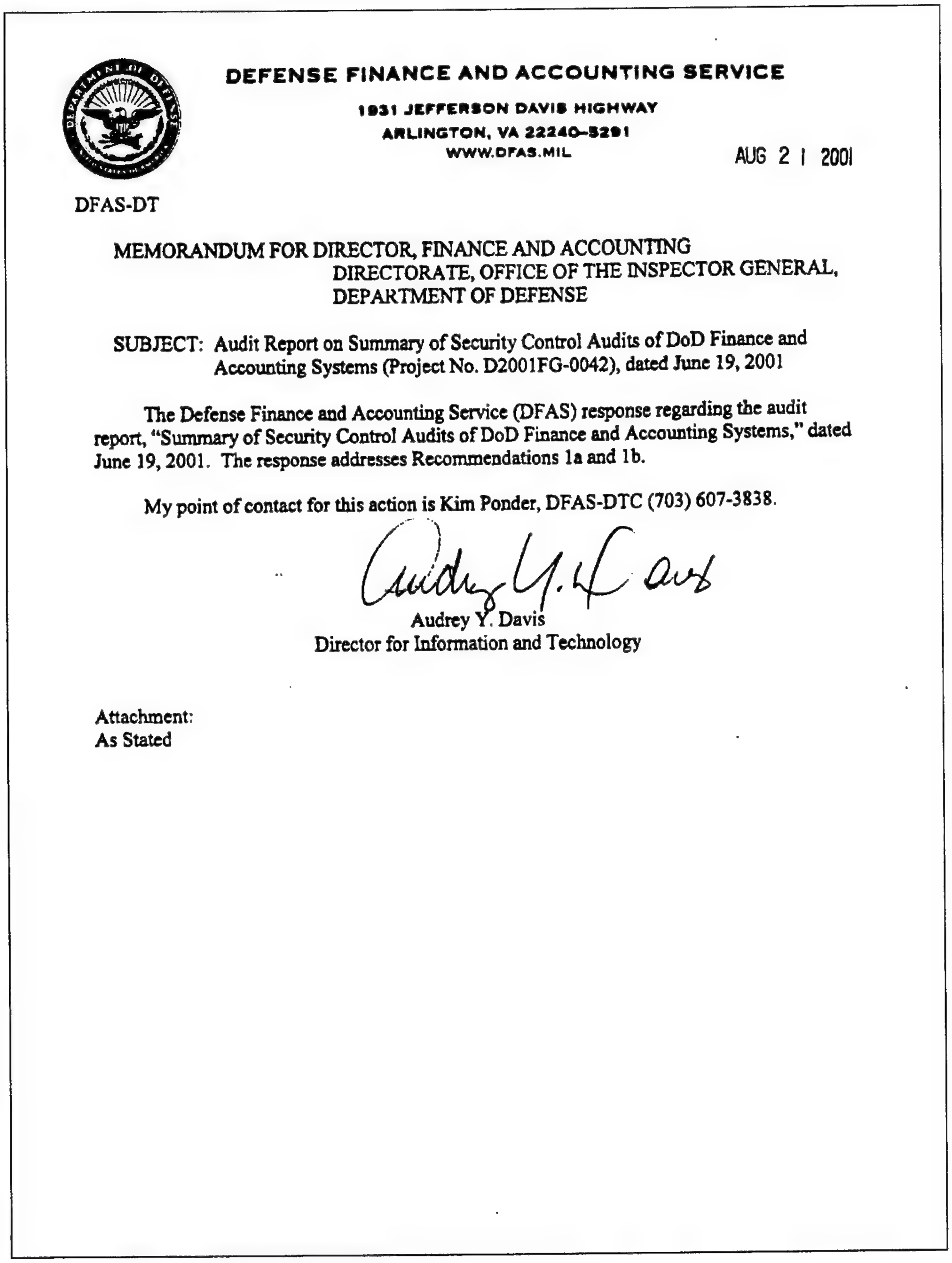
Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and International Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291
WWW.DFAS.MIL

AUG 2 1 2001

DFAS-DT

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

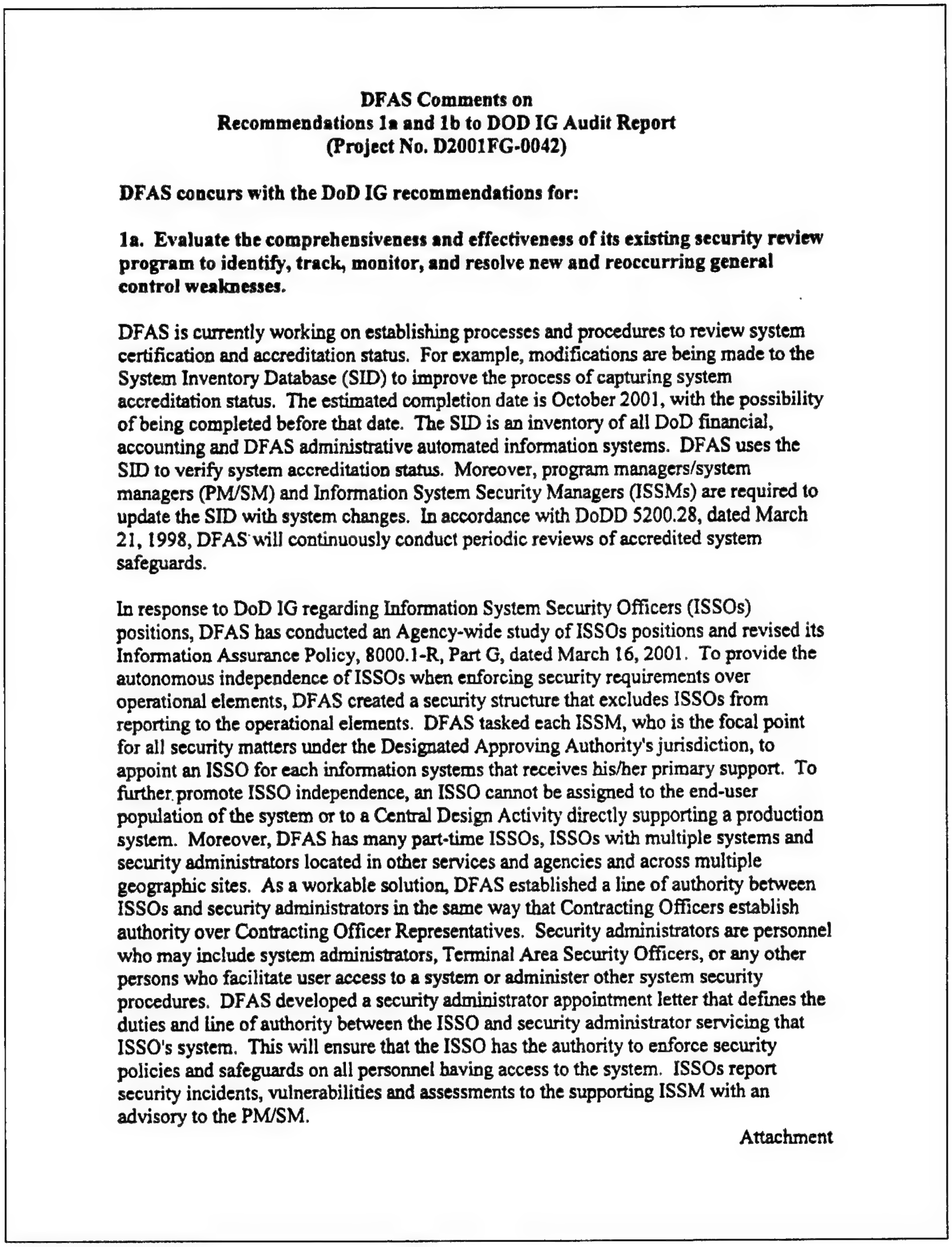
SUBJECT: Audit Report on Summary of Security Control Audits of DoD Finance and Accounting Systems (Project No. D2001FG-0042), dated June 19, 2001

The Defense Finance and Accounting Service (DFAS) response regarding the audit report, "Summary of Security Control Audits of DoD Finance and Accounting Systems," dated June 19, 2001. The response addresses Recommendations 1a and 1b.

My point of contact for this action is Kim Ponder, DFAS-DTC (703) 607-3838.

Audrey Y. Davis
Director for Information and Technology

Attachment:
As Stated



DFAS Comments on
Recommendations 1a and 1b to DOD IG Audit Report
(Project No. D2001FG-0042)

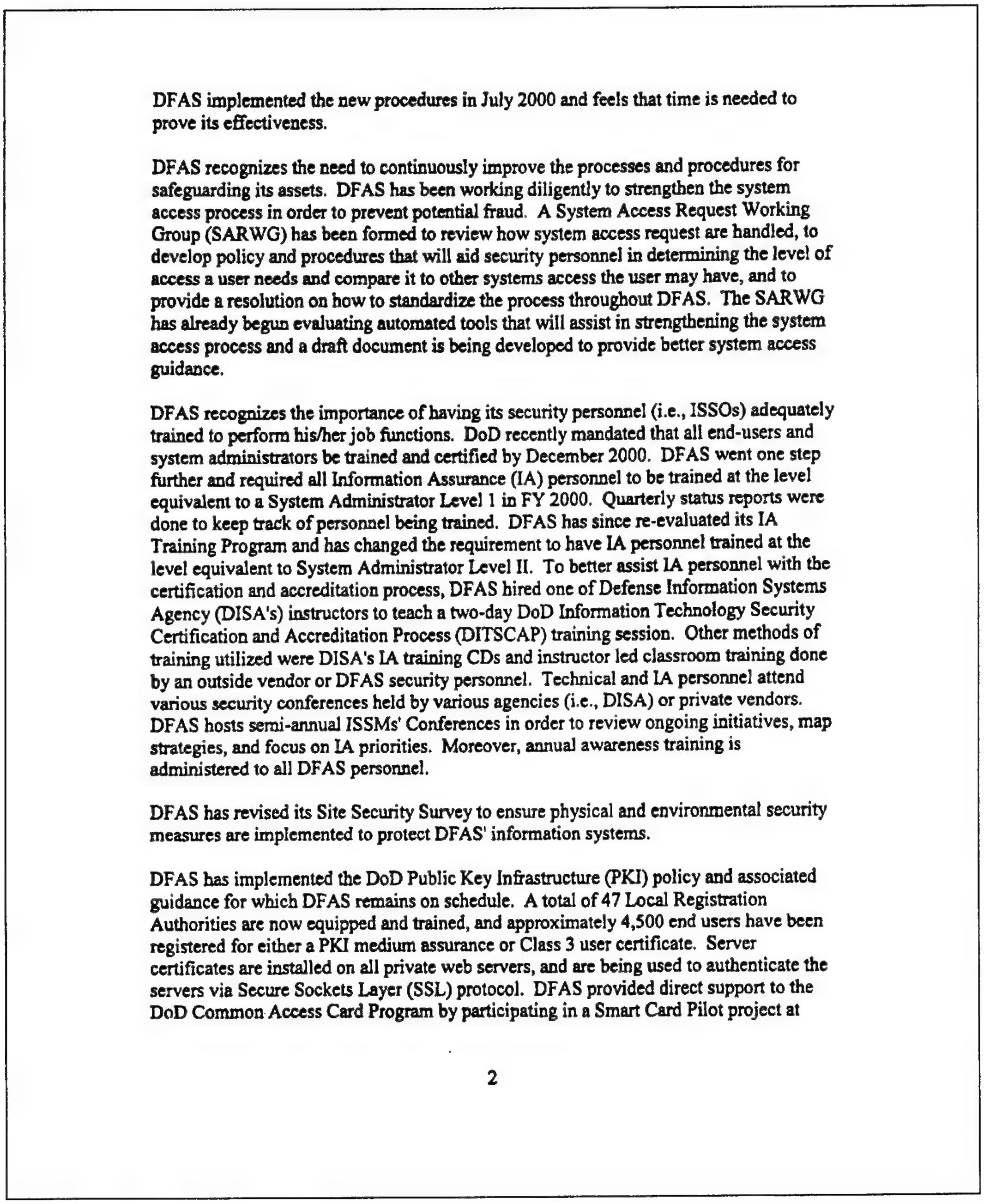
DFAS concurs with the DoD IG recommendations for:

1a. Evaluate the comprehensiveness and effectiveness of its existing security review program to identify, track, monitor, and resolve new and reoccurring general control weaknesses.

DFAS is currently working on establishing processes and procedures to review system certification and accreditation status. For example, modifications are being made to the System Inventory Database (SID) to improve the process of capturing system accreditation status. The estimated completion date is October 2001, with the possibility of being completed before that date. The SID is an inventory of all DoD financial, accounting and DFAS administrative automated information systems. DFAS uses the SID to verify system accreditation status. Moreover, program managers/system managers (PM/SM) and Information System Security Managers (ISSMs) are required to update the SID with system changes. In accordance with DoDD 5200.28, dated March 21, 1998, DFAS will continuously conduct periodic reviews of accredited system safeguards.

In response to DoD IG regarding Information System Security Officers (ISSOs) positions, DFAS has conducted an Agency-wide study of ISSOs positions and revised its Information Assurance Policy, 8000.1-R, Part G, dated March 16, 2001. To provide the autonomous independence of ISSOs when enforcing security requirements over operational elements, DFAS created a security structure that excludes ISSOs from reporting to the operational elements. DFAS tasked each ISSM, who is the focal point for all security matters under the Designated Approving Authority's jurisdiction, to appoint an ISSO for each information systems that receives his/her primary support. To further promote ISSO independence, an ISSO cannot be assigned to the end-user population of the system or to a Central Design Activity directly supporting a production system. Moreover, DFAS has many part-time ISSOs, ISSOs with multiple systems and security administrators located in other services and agencies and across multiple geographic sites. As a workable solution, DFAS established a line of authority between ISSOs and security administrators in the same way that Contracting Officers establish authority over Contracting Officer Representatives. Security administrators are personnel who may include system administrators, Terminal Area Security Officers, or any other persons who facilitate user access to a system or administer other system security procedures. DFAS developed a security administrator appointment letter that defines the duties and line of authority between the ISSO and security administrator servicing that ISSO's system. This will ensure that the ISSO has the authority to enforce security policies and safeguards on all personnel having access to the system. ISSOs report security incidents, vulnerabilities and assessments to the supporting ISSM with an advisory to the PM/SM.

Attachment



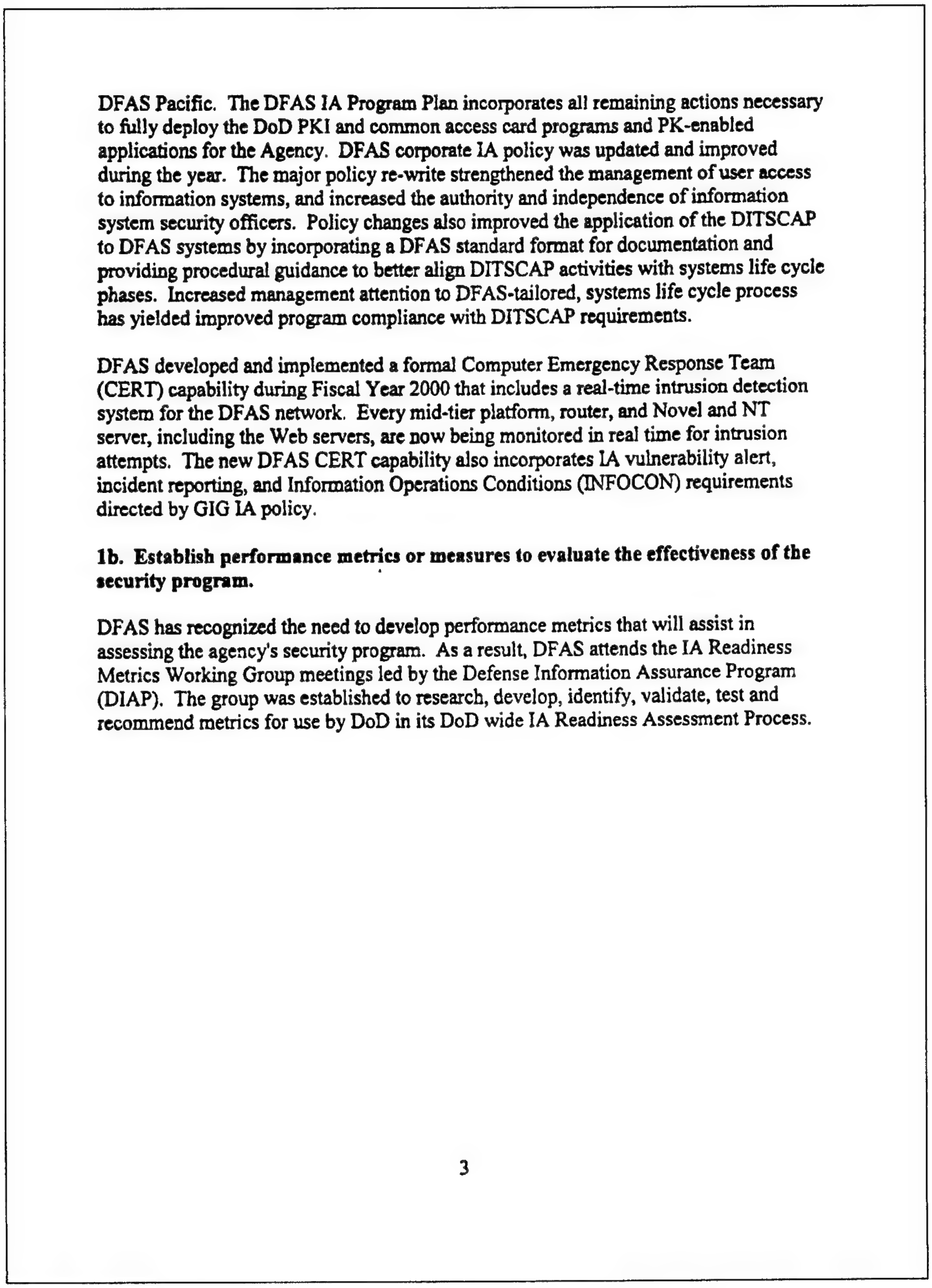
DFAS implemented the new procedures in July 2000 and feels that time is needed to prove its effectiveness.

DFAS recognizes the need to continuously improve the processes and procedures for safeguarding its assets. DFAS has been working diligently to strengthen the system access process in order to prevent potential fraud. A System Access Request Working Group (SARWG) has been formed to review how system access request are handled, to develop policy and procedures that will aid security personnel in determining the level of access a user needs and compare it to other systems access the user may have, and to provide a resolution on how to standardize the process throughout DFAS. The SARWG has already begun evaluating automated tools that will assist in strengthening the system access process and a draft document is being developed to provide better system access guidance.

DFAS recognizes the importance of having its security personnel (i.e., ISSOs) adequately trained to perform his/her job functions. DoD recently mandated that all end-users and system administrators be trained and certified by December 2000. DFAS went one step further and required all Information Assurance (IA) personnel to be trained at the level equivalent to a System Administrator Level 1 in FY 2000. Quarterly status reports were done to keep track of personnel being trained. DFAS has since re-evaluated its IA Training Program and has changed the requirement to have IA personnel trained at the level equivalent to System Administrator Level II. To better assist IA personnel with the certification and accreditation process, DFAS hired one of Defense Information Systems Agency (DISA's) instructors to teach a two-day DoD Information Technology Security Certification and Accreditation Process (DITSCAP) training session. Other methods of training utilized were DISA's IA training CDs and instructor led classroom training done by an outside vendor or DFAS security personnel. Technical and IA personnel attend various security conferences held by various agencies (i.e., DISA) or private vendors. DFAS hosts semi-annual ISSMs' Conferences in order to review ongoing initiatives, map strategies, and focus on IA priorities. Moreover, annual awareness training is administered to all DFAS personnel.

DFAS has revised its Site Security Survey to ensure physical and environmental security measures are implemented to protect DFAS' information systems.

DFAS has implemented the DoD Public Key Infrastructure (PKI) policy and associated guidance for which DFAS remains on schedule. A total of 47 Local Registration Authorities are now equipped and trained, and approximately 4,500 end users have been registered for either a PKI medium assurance or Class 3 user certificate. Server certificates are installed on all private web servers, and are being used to authenticate the servers via Secure Sockets Layer (SSL) protocol. DFAS provided direct support to the DoD Common Access Card Program by participating in a Smart Card Pilot project at



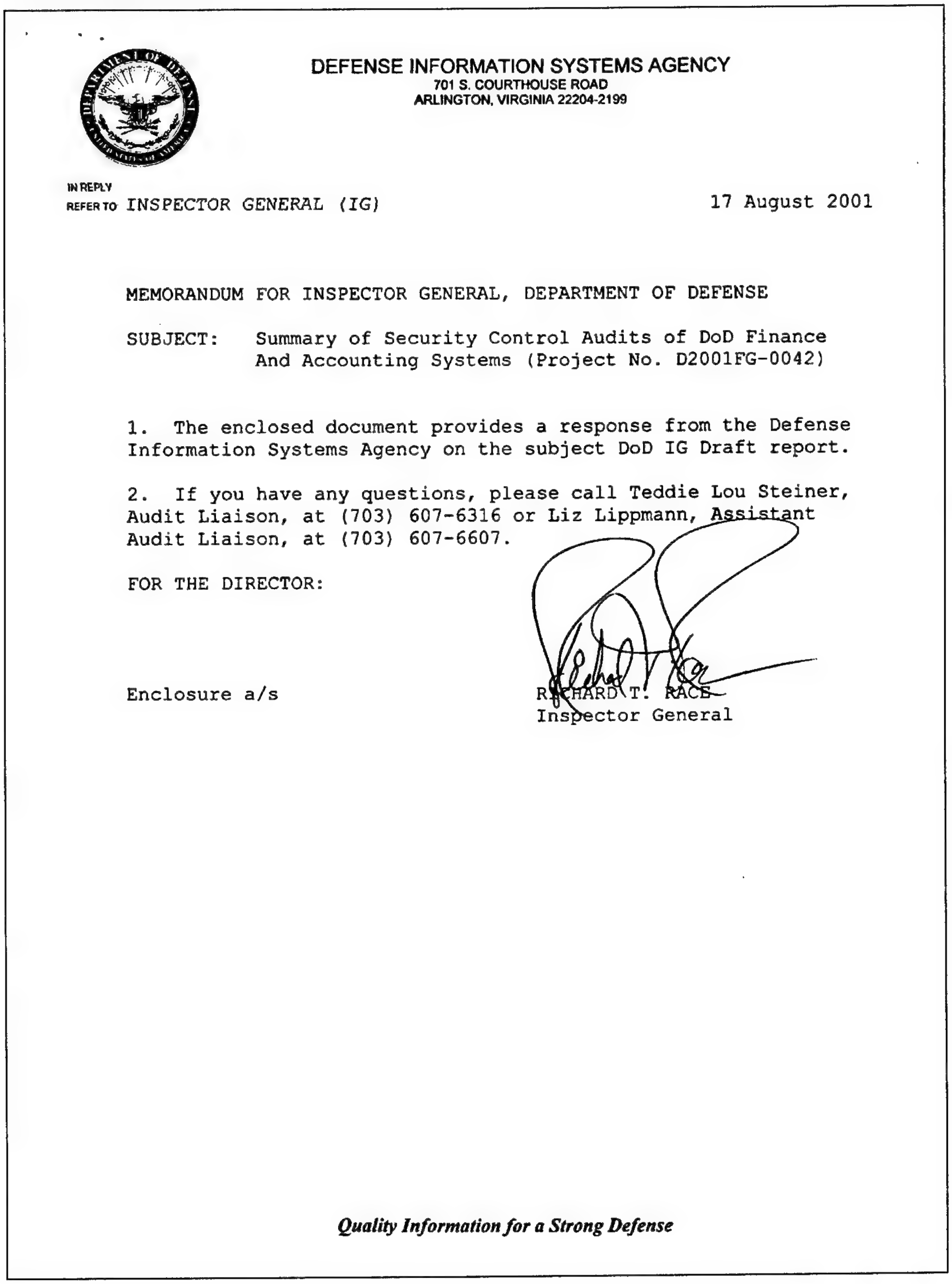
DFAS Pacific. The DFAS IA Program Plan incorporates all remaining actions necessary to fully deploy the DoD PKI and common access card programs and PK-enabled applications for the Agency. DFAS corporate IA policy was updated and improved during the year. The major policy re-write strengthened the management of user access to information systems, and increased the authority and independence of information system security officers. Policy changes also improved the application of the DITSCAP to DFAS systems by incorporating a DFAS standard format for documentation and providing procedural guidance to better align DITSCAP activities with systems life cycle phases. Increased management attention to DFAS-tailored, systems life cycle process has yielded improved program compliance with DITSCAP requirements.

DFAS developed and implemented a formal Computer Emergency Response Team (CERT) capability during Fiscal Year 2000 that includes a real-time intrusion detection system for the DFAS network. Every mid-tier platform, router, and Novel and NT server, including the Web servers, are now being monitored in real time for intrusion attempts. The new DFAS CERT capability also incorporates IA vulnerability alert, incident reporting, and Information Operations Conditions (INFOCON) requirements directed by GIG IA policy.

1b. Establish performance metrics or measures to evaluate the effectiveness of the security program.

DFAS has recognized the need to develop performance metrics that will assist in assessing the agency's security program. As a result, DFAS attends the IA Readiness Metrics Working Group meetings led by the Defense Information Assurance Program (DIAP). The group was established to research, develop, identify, validate, test and recommend metrics for use by DoD in its DoD wide IA Readiness Assessment Process.

Defense Information Systems Agency Comments



DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO INSPECTOR GENERAL (IG)

17 August 2001

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Summary of Security Control Audits of DoD Finance And Accounting Systems (Project No. D2001FG-0042)

1. The enclosed document provides a response from the Defense Information Systems Agency on the subject DoD IG Draft report.

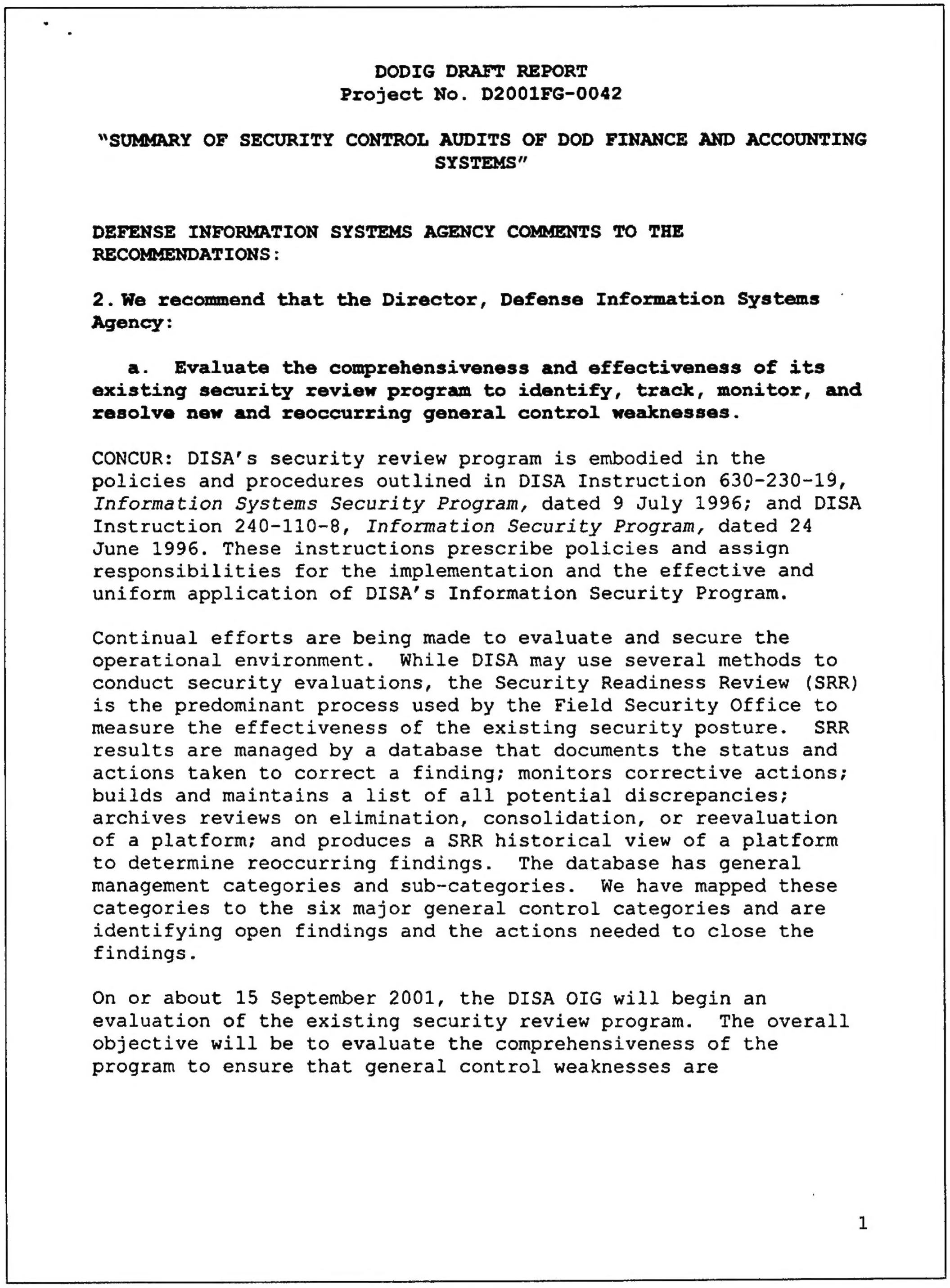
2. If you have any questions, please call Teddie Lou Steiner, Audit Liaison, at (703) 607-6316 or Liz Lippmann, Assistant Audit Liaison, at (703) 607-6607.

FOR THE DIRECTOR:

Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense



DODIG DRAFT REPORT
Project No. D2001FG-0042

"SUMMARY OF SECURITY CONTROL AUDITS OF DOD FINANCE AND ACCOUNTING SYSTEMS"

DEFENSE INFORMATION SYSTEMS AGENCY COMMENTS TO THE RECOMMENDATIONS:

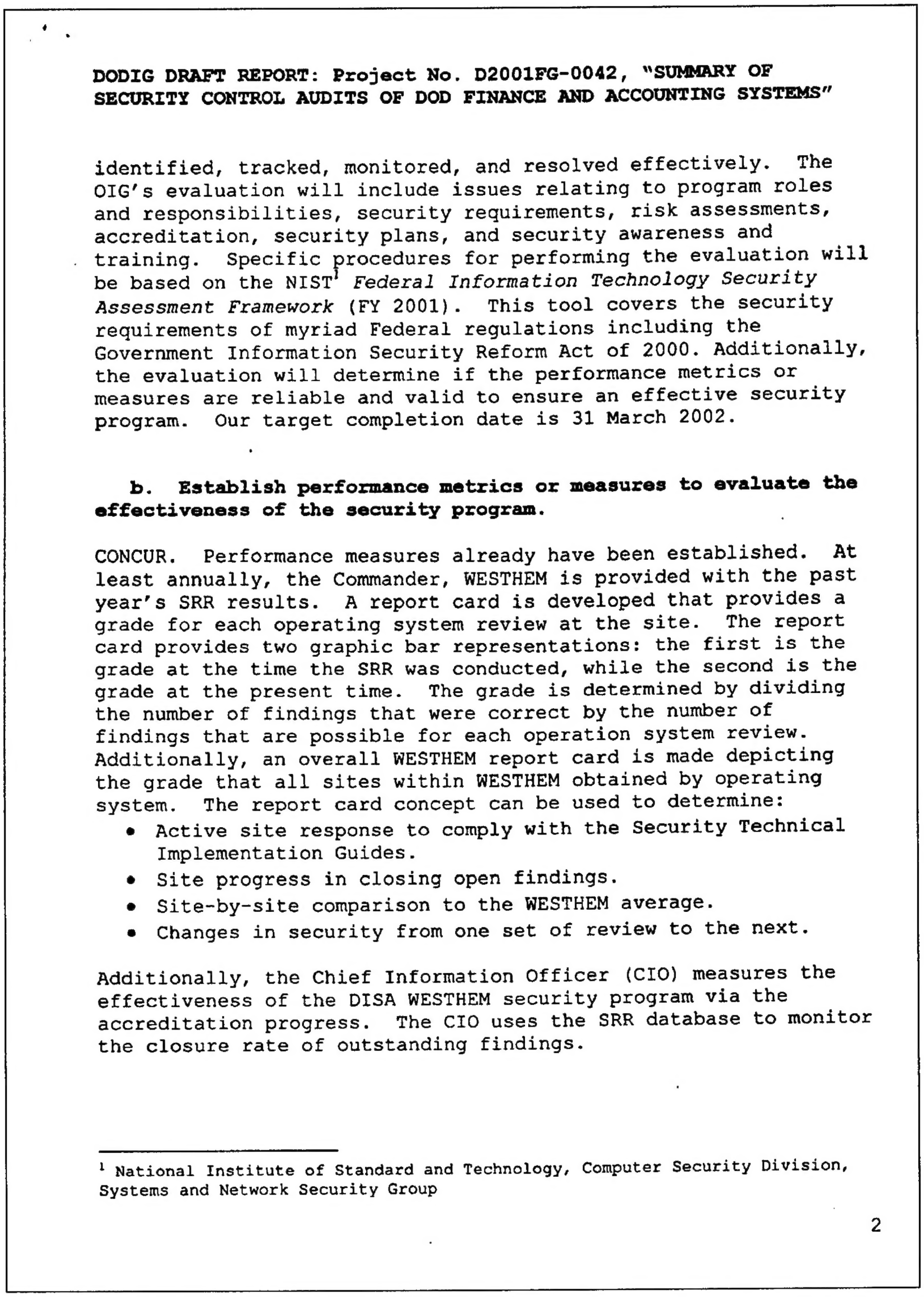
2. We recommend that the Director, Defense Information Systems Agency:

a. Evaluate the comprehensiveness and effectiveness of its existing security review program to identify, track, monitor, and resolve new and reoccurring general control weaknesses.

CONCUR: DISA's security review program is embodied in the policies and procedures outlined in DISA Instruction 630-230-19, *Information Systems Security Program,* dated 9 July 1996; and DISA Instruction 240-110-8, *Information Security Program,* dated 24 June 1996. These instructions prescribe policies and assign responsibilities for the implementation and the effective and uniform application of DISA's Information Security Program.

Continual efforts are being made to evaluate and secure the operational environment. While DISA may use several methods to conduct security evaluations, the Security Readiness Review (SRR) is the predominant process used by the Field Security Office to measure the effectiveness of the existing security posture. SRR results are managed by a database that documents the status and actions taken to correct a finding; monitors corrective actions; builds and maintains a list of all potential discrepancies; archives reviews on elimination, consolidation, or reevaluation of a platform; and produces a SRR historical view of a platform to determine reoccurring findings. The database has general management categories and sub-categories. We have mapped these categories to the six major general control categories and are identifying open findings and the actions needed to close the findings.

On or about 15 September 2001, the DISA OIG will begin an evaluation of the existing security review program. The overall objective will be to evaluate the comprehensiveness of the program to ensure that general control weaknesses are



identified, tracked, monitored, and resolved effectively. The OIG's evaluation will include issues relating to program roles and responsibilities, security requirements, risk assessments, accreditation, security plans, and security awareness and training. Specific procedures for performing the evaluation will be based on the NIST[1] *Federal Information Technology Security Assessment Framework* (FY 2001). This tool covers the security requirements of myriad Federal regulations including the Government Information Security Reform Act of 2000. Additionally, the evaluation will determine if the performance metrics or measures are reliable and valid to ensure an effective security program. Our target completion date is 31 March 2002.

b. Establish performance metrics or measures to evaluate the effectiveness of the security program.

CONCUR. Performance measures already have been established. At least annually, the Commander, WESTHEM is provided with the past year's SRR results. A report card is developed that provides a grade for each operating system review at the site. The report card provides two graphic bar representations: the first is the grade at the time the SRR was conducted, while the second is the grade at the present time. The grade is determined by dividing the number of findings that were correct by the number of findings that are possible for each operation system review. Additionally, an overall WESTHEM report card is made depicting the grade that all sites within WESTHEM obtained by operating system. The report card concept can be used to determine:

- Active site response to comply with the Security Technical Implementation Guides.
- Site progress in closing open findings.
- Site-by-site comparison to the WESTHEM average.
- Changes in security from one set of review to the next.

Additionally, the Chief Information Officer (CIO) measures the effectiveness of the DISA WESTHEM security program via the accreditation progress. The CIO uses the SRR database to monitor the closure rate of outstanding findings.

[1] National Institute of Standard and Technology, Computer Security Division, Systems and Network Security Group

Summary Report Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector, DoD, who contributed to the report are listed below.

Paul J. Granetto
Marvin L. Peek
Kathryn M. Truex
Dennis L. Conway
Margaret B. Bennardo
David P. Yarrington

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Summary of Security Control Audits of DOD Finance and Accounting Systems

B. DATE Report Downloaded From the Internet: 11/27/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 11/27/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.